

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of )

(Briefly describe the property to be searched  
or identify the person by name and address) )

Case No. 25-M-308 (WEC)

Information associated with the cellular device )  
assigned call number 847-313-5738 in the )  
custody or control of Verizon Wireless )

## WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the \_\_\_\_\_ District of \_\_\_\_\_ New Jersey  
(identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before January 22, 2025 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

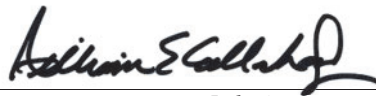
The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to \_\_\_\_\_

(United States Magistrate Judge)

☒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)☒ for 30 days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_

Date and time issued:

1/8/25, 3:30 p.m.



Judge's signature

City and state:

Milwaukee, WI

U.S. Magistrate Judge William E. Callahan

Printed name and title

<b>Return</b>		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
<b>Certification</b>		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

## **ATTACHMENT A**

### **Property to be Searched**

This warrant applies to records and information associated with the cellular device assigned **847-313-5738** (the “Subject Account” or “Target Cell Phone”) that is in the custody or control of **Verizon Wireless** (“Service Provider”) a wireless communications service provider that is headquartered at 180 Washington Valley Road, Bedminster, NJ 07921.

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be Disclosed by the Provider**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Service Provider, including any information that has been deleted but is still available to the Service Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Service Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

- a. The following subscriber and historical information about the customers or subscribers associated with the Subject Account for the time period 11/01/2024-1/8/2025:
  - i. Names (including subscriber names, user names, and screen names);
  - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
  - iii. Local and long distance telephone connection records;
  - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
  - v. Length of service (including start date) and types of service utilized;
  - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

- vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
- viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.
- ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Subject Account including:

(A) the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

(ii) information regarding the cell tower and antenna face (also known as "sectors") through which the communications were sent and received as well as per-call measurement data (also known as "real-time tool" or "RTT").

- b. Information associated with each communication to and from the SUBJECT ACCOUNT for a period of 30 days from the date of this warrant, including:

- i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;
- ii. Source and destination telephone numbers;
- iii. Date, time, and duration of communication; and
- iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which the SUBJECT PHONE will connect at the beginning and end of each

communication as well as per-call measurement data (also known as “real-time tool” or “RTT”).

The Court has also issued an order pursuant to 18 U.S.C. § 3123, dated today, for such information associated with the Target Cell Phone.

- c. Information about the location of the Target Cell Phone for a period of 30 days, during all times of day and night. “Information about the location of the Target Cell Phone” includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information.
  - i. To the extent that the information described in the previous paragraph (“Location Information”) is within the possession, custody, or control of the Service Provider, the Service Provider is required to disclose the Location Information to the government. In addition, the Service Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with the Service Provider’s services, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider’s network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.
  - ii. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

## **II. Information to be Seized by the Government**

All information described in Section I that will assist in arresting Mateusz Panszczyk who was charged with violating 18 U.S.C. § 371 on December 10, 2024, and

is a “person to be arrested” within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.

## UNITED STATES DISTRICT COURT

for the  
Eastern District of WisconsinIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)Information associated with the cellular device  
assigned call number 847-313-5738 in the custody or  
control of Verizon WirelessCase No. **25-M-308 (WEC)****APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the \_\_\_\_\_ District of New Jersey, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☐ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
18 U.S.C. § 371Offense Description  
Arrest warrant is based on violations of 18 U.S.C. § 371 (Conspiracy to Transport Stolen Goods Interstate and Conspiracy to Possess or Receive Stolen Goods in violation of 18 U.S.C. §§ 2314 & 2315)

The application is based on these facts:

See Attached Affidavit

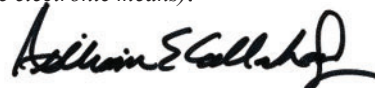
- ☒ Continued on the attached sheet.
- ☒ Delayed notice of 30 days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

**GARY M ROY**Digitally signed by GARY M ROY  
Date: 2025.01.08 11:54:57 -06'00'

Applicant's signature

Gary Roy, Deputy USM, USMS

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
\_\_\_\_\_  
Telephone (specify reliable electronic means).Date: 1/8/25

Judge's signature

City and state: Milwaukee, WI**Hon. William E. Callahan, Jr.**

Printed name and title



**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Gary Roy, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) and Federal Rule of Criminal Procedure 41 for information associated with a certain cellular device assigned call number 847-313-5738 (“Subject Account” or “Target Cell Phone”) that is in the custody or control of Verizon Wireless, a wireless communication service provider that is headquartered at 180 Washington Valley Road, Bedminster, NJ 07921. As a provider of wireless communications service, Verizon Wireless is a provider of an electronic communications service, as defined in 18 U.S.C. § 2510(15). The Subject Account is described herein and in Attachment A, and the information to be seized is described herein and in Attachment B.

2. Because this warrant seeks the prospective collections of information, including cell-site location information, that may fall within statutory definitions of information collected by a “pen register” and/or “trap and trace device,” *see* 18 U.S.C. § 3127(3) & (4), I also make this affidavit in support of an application by the United States of America for an order pursuant to 18 U.S.C. §§ 3122 and 3123, authorizing the installation and use of pen registers and trap and trace devices (“pen-trap devices”) to record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to or from the Target Cell Phone.

3. I am a Deputy United States Marshal with the United States Marshals Service ("USMS"), acting as a Task Force Officer ("TFO") currently assigned to the Eastern Wisconsin Violent Offender Task Force ("EWVOTF") and, as such, am charged with enforcing all laws in all jurisdictions of the United States, its territories and possessions. I have been a member of the EWVOTF since February 2023 and have investigated multiple fugitive cases. I have had both formal training and have participated in numerous investigations to locate federal and state fugitives. I am an investigator or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), in that I am empowered by law to conduct investigations of and to make arrests for federal felony offenses. I am also employed as a Special Agent with Homeland Security Investigations ("HSI") and have been so employed since February 2018. Prior to my employment at HSI, I was employed as a Patrol Agent with the United States Border Patrol since December 2007. To date, I have approximately seventeen years of law enforcement experience.

4. The facts in this affidavit come from my personal observations, my training and experience, my review of documents, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that Mateusz PANSZCZYK ("PANSZCZYK") has violated 18 U.S.C. § 371 (Conspiracy to Transport Stolen Goods Interstate and Conspiracy to Possess or Receive

Stolen Goods in violation of 18 U.S.C. §§ 2314 & 2315). PANSZCZYK was originally charged via criminal complaint on or about November 12, 2024, and then he was indicted for this crime on December 10, 2024, by a grand jury sitting in the Eastern District of Wisconsin. He was originally subject to an arrest warrant issued on November 12, 2024, in case number 24-MJ-522, but that arrest warrant has been superseded by an arrest warrant issued on December 11, 2024, in case number 24-CR-226. There is also probable cause to believe that the location information described in Attachment B will assist law enforcement in arresting PANSZCZYK, who is a “person to be arrested” within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

6. The court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the court is a district court of the United States that has jurisdiction over the offense being investigated. *See* 18 U.S.C. § 2711(3)(A)(i).

#### **PROBABLE CAUSE**

7. The United States government, including the USMS, is conducting a fugitive investigation of PANSZCZYK who is currently wanted for violations of Title 18, United States Code, Section 371 (Conspiracy to Transport Stolen Goods Interstate and Conspiracy to Possess or Receive Stolen Goods in violation of 18 U.S.C. §§ 2314 & 2315).

8. On November 12, 2024, PANSZCZYK and three other co-conspirators were charged by criminal complaint in the Eastern District of Wisconsin for violations of Title 18, United States Code, Section 371 (Conspiracy to Transport Stolen Goods

Interstate and Conspiracy to Possess or Receive Stolen Goods in violation of 18 U.S.C. §§ 2314 & 2315) in Case No. 24-MJ-522. Arrest warrants for all four individuals including PANSZCZYK were issued simultaneously. Additionally, search warrants for three locations including PANSZCZYK's residence were authorized the same day.

9. On November 14, 2024, HSI Special Agents (SAs), along with other law enforcement partners executed the aforementioned search warrants and attempted to serve the arrest warrant on PANSZCZYK at his residence (21225 116th St, Bristol, WI 53104). A search of the residence revealed PANSZCZYK was not present. During the execution of the search warrant, law enforcement officers encountered Janina Panszczyk. Janina Panszczyk identified herself as PANSZCZYK's mother and told law enforcement officers she had not seen her son in a while. In the days prior to the execution of the search warrant, however, law enforcement officers observed PANSZCZYK at the residence.

10. On December 10, 2024, a grand jury sitting in the Eastern District of Wisconsin indicted PANSZCZYK and his three other co-conspirators for violations of Title 18, United States Code, Section 371 (Conspiracy to Transport Stolen Goods Interstate and Conspiracy to Possess or Receive Stolen Goods in violation of 18 U.S.C. §§ 2314 & 2315) (Case No. 24-CR-226). A new arrest warrant was issued for PANSZCZYK on December 11, 2024.

11. The investigation into PANSZCZYK for conspiring to transport stolen goods interstate and to possess or receive stolen goods revealed that he utilized two numbers, namely 262-995-3412 and 847-313-5738, the Subject Account. For example, on

November 14, 2024, law enforcement interviewed PANSZCZYK's cousin, Sebastian Panszczyk, who indicated PANSZCZYK's phone number was 262-995-3412. On the same day, law enforcement interviewed a possible girlfriend of PANSZCZYK and her sister. They both indicated that PANSZCZYK's phone number was 847-313-5738. One of PANSZCZYK's employees indicated through his attorney that PANSZCZYK had two phone numbers 262-995-3412 and 847-313-5738.

12. Database queries show the Subject Account's carrier to be Verizon Wireless. On November 27, 2024, I issued a Department of Homeland Security (DHS) Subpoena to Verizon Wireless requesting information associated with the Subject Account. Verizon Wireless provided a response from July 1, 2024 through November 25, 2024, and I observed the Target Cell Phone's subscriber is listed as Janina Panszczyk, PANSZCZYK's mother, out of 21225 116<sup>th</sup> St, Bristol, WI 53104.

13. The response from Verizon Wireless also included call records which details the incoming/outgoing calls for the Subject Account. I reviewed the provided records and generated a frequency report to identify phone numbers most frequently communicating with the Subject Account. Records for the whole time period show among the most frequently called numbers are those belonging to Janina Panszczyk, PANSZCZYK's mother, and Paulina Panszczyk, previously identified as PANSZCZYK's sister. I also observed that there were numerous entries indicating that the Subject Account was potentially receiving calls from November 15 to November 24, 2024 (after the search warrant was executed on his residence). Accordingly, based on

my training and experience, the Subject Account has not been dropped and will still be useful in locating PANSZCZYK.

14. Based on my training and experience in locating and apprehending fugitives, the data being sought by this warrant will assist in locating PANSZCZYK. Because successful apprehensions often rely on the element of surprise and on taking the fugitive unawares, it is often necessary to attempt an arrest during nighttime or the early morning hours, when most people are sleeping. Further, apprehension tactical plans often change at the last minute based on unexpected movements or other behavior of the target. Therefore, I cannot predict in advance when this data would need to be accessed and would need access to the data at all times of the day or night in order to ensure a safe and successful apprehension.

15. As of the date of this affidavit, PANSZCZYK's whereabouts remain unknown, and the arrest warrant in case number 24-CR-226 remains unserved.

16. In my training and experience, I have learned that Verizon Wireless is a company that provides cellular communications service to the general public. I also know that providers of cellular communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they provide service, including cell-site data, also known as "tower/face information" or cell tower/sector records. Cell-site data identifies the "cell towers" (*i.e.*, antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the "sector" (*i.e.*, faces of the towers)

to which the device connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate general location of the cellular device.

17. Based on my training and experience, I know that Verizon Wireless can collect cell-site data on a prospective basis about the Subject Account. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as Verizon Wireless typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

18. Based on my training and experience, I know that Verizon also can collect per-call measurement data, which Verizon also refers to as the “real-time tool” (“RTT”). RTT data estimates the approximate distance of the cellular device from a cellular tower based upon the speed with which signals travel between the device and the tower. This information can be used to estimate an approximate location range that is more precise than typical cell-site data.

19. Based on my training and experience, I know that Verizon Wireless has the technical capabilities that allow them to collect and generate E-911 Phase II data, also known as GPS data or latitude-longitude data. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. I know that Verizon Wireless can collect E-911 Phase II data about the location of the Target Cell Phone, including by initiating a signal to determine the location of the Target Cell Phone on Verizon Wireless's network or with such other reference points as may be reasonably available.

20. Based on my training and experience, I know each cellular device has one or more unique identifiers embedded inside it. Depending on the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), a Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Equipment Identity ("IMEI"). The unique identifiers – as transmitted from a cellular device to a cellular antenna or tower – can be recorded by pen-trap devices and indicate the identity of the cellular device making the communication without revealing the communication's content.

21. Based on my training and experience, I know that wireless providers such as Verizon Wireless typically collect and retain information about their subscribers in



their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the methods of payment (such as credit card account number) provided by the subscriber to pay for wireless communication service. I also know that wireless providers such as Verizon Wireless typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular device and other transactional records, in their normal course of business.

#### **AUTHORIZATION REQUEST**

22. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

23. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the Target Cell Phone would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to change patterns of behavior and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant

authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

24. I further request that the Court direct Verizon Wireless to disclose to the government any information described in Attachment B that is within the possession, custody, or control of Verizon Wireless. I also request that the Court direct Verizon Wireless to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with Verizon Wireless's services, including by initiating a signal to determine the location of the Target Cell Phone on Verizon Wireless's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate Verizon Wireless for reasonable expenses incurred in furnishing such facilities or assistance.

25. Because the warrant will be served on Verizon Wireless, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night. I further request that the Court authorize the execution of the warrant at any time of day or night, owing to the potential need to locate the Target Cell Phone outside of daytime hours.

## **ATTACHMENT A**

### **Property to be Searched**

This warrant applies to records and information associated with the cellular device assigned **847-313-5738** (the “Subject Account” or “Target Cell Phone”) that is in the custody or control of **Verizon Wireless** (“Service Provider”) a wireless communications service provider that is headquartered at 180 Washington Valley Road, Bedminster, NJ 07921.

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be Disclosed by the Provider**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Service Provider, including any information that has been deleted but is still available to the Service Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Service Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

- a. The following subscriber and historical information about the customers or subscribers associated with the Subject Account for the time period 11/01/2024-1/8/2025:
  - i. Names (including subscriber names, user names, and screen names);
  - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
  - iii. Local and long distance telephone connection records;
  - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
  - v. Length of service (including start date) and types of service utilized;
  - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

- vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
- viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.
- ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Subject Account including:

(A) the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

(ii) information regarding the cell tower and antenna face (also known as "sectors") through which the communications were sent and received as well as per-call measurement data (also known as "real-time tool" or "RTT").

- b. Information associated with each communication to and from the SUBJECT ACCOUNT for a period of 30 days from the date of this warrant, including:

- i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;
- ii. Source and destination telephone numbers;
- iii. Date, time, and duration of communication; and
- iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which the SUBJECT PHONE will connect at the beginning and end of each

communication as well as per-call measurement data (also known as “real-time tool” or “RTT”).

The Court has also issued an order pursuant to 18 U.S.C. § 3123, dated today, for such information associated with the Target Cell Phone.

- c. Information about the location of the Target Cell Phone for a period of 30 days, during all times of day and night. “Information about the location of the Target Cell Phone” includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information.
  - i. To the extent that the information described in the previous paragraph (“Location Information”) is within the possession, custody, or control of the Service Provider, the Service Provider is required to disclose the Location Information to the government. In addition, the Service Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with the Service Provider’s services, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider’s network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.
  - ii. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

## **II. Information to be Seized by the Government**

All information described in Section I that will assist in arresting Mateusz Panszczyk who was charged with violating 18 U.S.C. § 371 on December 10, 2024, and

is a “person to be arrested” within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.